Lecture 11: Internetworking and the Internet Protocol (IP)

Dr. Mohammed Hawa
Electrical Engineering Department
University of Jordan

Network vs. Internetwork

• Interconnected hosts running the same data link layer protocol represent one physical network.
• A physical network is usually controlled by a single administrative entity.
• Different physical networks exist to fit different set of needs (e.g., wired vs. wireless). No single networking technology fits the needs of all users.
• An internetwork connects the different networks instead of being isolated islands, which allow information exchange.
• The Internet is a global internetwork (not network).
### The Internetworking Concept: The Network Layer

<table>
<thead>
<tr>
<th>L3</th>
<th>Network Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2</td>
<td>LLC</td>
</tr>
<tr>
<td>MAC</td>
<td>MAC</td>
</tr>
<tr>
<td>L1</td>
<td>PHY</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Wi-Fi</td>
</tr>
</tbody>
</table>

### Network Layer solves 3 issues:

1. Provides a *homogeneous* addressing scheme that is *globally unique*: Different L2 protocols might use different sizes (number of bits) for their MAC addresses. LAA addresses might be re-used on different networks (no guarantees).

2. Provides a *uniform* packet format. Different L2 protocols might use different sizes for their frames, and might include different fields in the header depending on the protocol design.

3. Defines *end-to-end* routing across multiple physical networks (through routers): A huge self-learning table in each switch for the *whole* world is not feasible, plus flooding to all machines in the world from one PC consumes excessive resources.
Internet Protocol (IP)

- The IP protocol is the *de facto* L3 protocol nowadays.
- IP is currently in its version 4, called IPv4, described in IETF RFC 791 (published 1981).
- The next version is 6, called IPv6.
- IPv6 was first formally described in RFC 1883 (published 1995). That RFC was obsoleted and replaced by RFC 2460 (published 1998).
- This specification was obsoleted again and replaced by RFC 8200 (July 2017).
- Deployment of IPv6 was slow, but is picking up in recent years.
- Routers forward based on IP address (e.g., 128.2.1.1) not the MAC address.

IPv6 Deployment
IP Packet Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>A 4 bit field. The current version is 4 (0100b). The next version is 6 (0110b).</td>
</tr>
<tr>
<td>IP Header Length (IHL)</td>
<td>A 4 bit field. Specifies the length of the header, in units of 32-bit words.</td>
</tr>
<tr>
<td></td>
<td>Used because the header length is not constant. The minimum value is 5, and</td>
</tr>
<tr>
<td></td>
<td>the maximum value is 15, which limits the header to 60 bytes, and the</td>
</tr>
<tr>
<td></td>
<td>Options field to 40 bytes.</td>
</tr>
<tr>
<td>Type of Service</td>
<td>Used to distinguish quality of service desired for the packet (mainly used</td>
</tr>
<tr>
<td></td>
<td>for the Diffserv QoS architecture). It allows the router to decide on a</td>
</tr>
<tr>
<td></td>
<td>certain queueing priority and a discard priority for the received packet.</td>
</tr>
<tr>
<td></td>
<td>For voice, fast delivery is preferred. For file transfer, complete</td>
</tr>
<tr>
<td></td>
<td>transmission is more important.</td>
</tr>
</tbody>
</table>

Copyright © Dr. Mohammed Hawa  
Electrical Engineering Department, University of Jordan  
9/10
IP Packet Format

- **Total Length**: A 16-bit integer that specifies the total number of bytes in the packet (including both the header and the data). So, the maximum IP packet length is $2^{16} - 1 = 65,535$ bytes.

- **Identification, Flags and Fragment Offset**: used when the IP datagram is fragmented. All fragments of a single IP datagram contain the same identification.

- The MF flag stands for “More Fragments to follow”. All fragments of an IP datagram except the last one have this bit set.

- The DF flag stands for “Do not Fragment”. When a host does not want its IP packet to be fragmented, it sets this bit to 1.

- The Fragment Offset tells the receiver where in the current datagram the fragment belongs. All fragments in a datagram except the last one must be a multiple of 8 bytes.

- **Time to Live (TTL)**: A counter used to limit packet lifetime. It is initialized to a positive integer between 1 and 255 by the sender, and is decremented by 1 for each one hop. When the counter hits zero, the router discards the IP packet and sends an ICMP packet back to the source. (Usually: 128 or 255).
IP Packet Fields

- **Protocol**: A number that tells the receiver to which Layer 4 process to deliver data. Possibilities include TCP = 6, UDP = 17, ICMP = 1, etc.

- **Header Checksum**: used to detect errors in the header only. Note that the header checksum must be recomputed at each hop because at least one field always changes (the TTL field), but special tricks can be used to speed up the computation.

- **Source Address**: the IP address of the sender (a unique 32-bit number).

- **Destination Address**: IP address of the intended recipient (a unique 32-bit number).

- **Options**: provides an escape to include information not present in the original design, to permit experimenters to try out new ideas, and to avoid allocating header bits to information that is rarely used.
Internet Control Message Protocol (ICMP)

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESTINATION UNREACHABLE</td>
<td>Packet could not be delivered</td>
</tr>
<tr>
<td>TIME EXCEEDED</td>
<td>Time To Live (TTL) field hit 0</td>
</tr>
<tr>
<td>ECHO</td>
<td>Ask a machine if it is alive</td>
</tr>
<tr>
<td>ECHO REPLY</td>
<td>Yes, I am alive</td>
</tr>
</tbody>
</table>

Usage: ping domain_name or ping IP_address

C:\>ping www.google.com
Pinging www.l.google.com [74.125.77.147] with 32 bytes of data:
Reply from 74.125.77.147: bytes=32 time=264ms TTL=237
Reply from 74.125.77.147: bytes=32 time=199ms TTL=237
Reply from 74.125.77.147: bytes=32 time=188ms TTL=237
Reply from 74.125.77.147: bytes=32 time=195ms TTL=237
Ping statistics for 74.125.77.147:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 188ms, Maximum = 264ms, Average = 211ms

C:\>ping www.ju.edu.jo
Pinging webserver.ju.edu.jo [172.16.0.33] with 32 bytes of data:
Reply from 172.16.0.33: bytes=32 time<1ms TTL=127
Reply from 172.16.0.33: bytes=32 time<1ms TTL=127
Reply from 172.16.0.33: bytes=32 time<1ms TTL=127
Reply from 172.16.0.33: bytes=32 time<1ms TTL=127
Ping statistics for 172.16.0.33:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
Usage: `tracert domain_name` or `tracert IP_address`

C:\>tracert fetweb.ju.edu.jo [10.249.103.200]
Tracing route to fetweb.ju.edu.jo (10.249.103.200)
over a maximum of 30 hops:
1  <1 ms  <1 ms  <1 ms  10.249.103.200
Trace complete.

C:\>tracert www.ju.edu.jo [172.16.0.116]
Tracing route to www.ju.edu.jo (172.16.0.116)
over a maximum of 30 hops:
1  <1 ms  <1 ms  <1 ms  10.249.96.10
2  1149 ms 159 ms  21 ms  www.ju.edu.jo [172.16.0.116]
Trace complete.

C:\>tracert www.google.com
Tracing route to www.google.com [209.85.129.147]
over a maximum of 30 hops:
1   2 ms  <1 ms  <1 ms  192.168.1.10
2   619 ms 363 ms  483 ms  195.163.110.207
3   981 ns 980 ns 1268 ms  195.163.119.5
4  337 ms  563 ms  219.139.32.9
5  538 ms  734 ms  98 ms so-5-0-0.fra10.ip.tiscali.net [77.67.66.69]
6  309 ns 102 ms  191 ms xx-0-0-0.amx10.ip.tiscali.net [89.149.186.233]
7  118 ms 264 ms  131 ms corax.amx.net.google.com [195.69.146.247]
8  359 ms 244 ms  105 ms 209.85.248.88
9  126 ms 377 ms  149 ms 72.14.232.207
10  108 ms 111 ms  112 ms 72.14.233.206
11  275 ms 439 ms  417 ms 72.14.233.206
12  210 ms 406 ms  112 ms fk-in-f147.google.com [209.85.129.147]
Trace complete.

C:\>tracert www.microsoft.com
Tracing route to lb1.www.ms.akadns.net [207.46.192.254]
over a maximum of 30 hops:
1   <1 ms  <1 ms  1 ms  192.168.1.10
2   483 ms 902 ms  597 ms  195.163.110.207
3   309 ms 325 ms  337 ms  195.163.119.5
4   613 ms 366 ms  546 ms  219.139.32.9
5  359 ms 512 ms  138 ms so-5-0-0.fra10.ip.tiscali.net [77.67.66.69]
6  733 ms 450 ms  131 ms corax.amx.net.google.com [195.69.146.247]
7  850 ms 602 ms 1013 ms so-2-0-0.wst-64cb-1b.ntwk.msn.net [207.46.35.35]
8  904 ms 694 ms  821 ms ge-6-1-0-0.tuk-64cb-1b.ntwk.msn.net [207.46.35.35]
9  813 ms 768 ms  631 ms ge-7-1-0-0.wst-64cb-1b.ntwk.msn.net [207.46.35.247]
10  339 ms 261 ms  221 ms ge-0-0-0-0.wst-64cb-1b.ntwk.msn.net [207.46.35.247]
11  885 ms 691 ms  519 ms ge-7-1-0-0.wst-64cb-1b.ntwk.msn.net [207.46.35.35]
12  763 ms 694 ms  821 ms ge-6-1-0-0.tuk-64cb-1b.ntwk.msn.net [207.46.35.35]
13 1115 ms 741 ms  340 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
14  561 ms 516 ms  698 ms pol1.tuk-64cb-1b.ntwk.msn.net [207.46.35.122]
15  378 ms 325 ms  467 ms pol2.tuk-64cb-1b.ntwk.msn.net [207.46.35.122]
16  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
17  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
18  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
19  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
20  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
21  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
22  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
23  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
24  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
25  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
26  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
27  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
28  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
29  413 ms 490 ms  459 ms tskl-2.tuk-76cb-1b.ntwk.msn.net [207.46.35.50]
30  413 ms 490 ms  459 ms pol1.tuk-64cb-1b.ntwk.msn.net [207.46.35.138]
    reports: Destination net unreachable.
Trace complete.
Homework: Firewalls

- Read the Wikipedia entry for Firewall
  - [http://en.wikipedia.org/wiki/Firewall_(computing)]
- A firewall is classified as which layer device (e.g., a router is a L3 device)?
- How is a firewall different than a proxy?
- How did the JU firewall affect the above ping and traceroute entries?
- Try to use ping and traceroute inside and outside the University.
- What is a Gateway? Which layer device is it?

Networking Devices

<table>
<thead>
<tr>
<th>Layer</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7</td>
<td>Firewall, Proxy, Gateway</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Router</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Switch, Bridge</td>
</tr>
<tr>
<td>Layer 1</td>
<td>Hub, Repeater</td>
</tr>
</tbody>
</table>